Unit 2: Computing Security Concepts and Problems 2

[The CIA Model](https://courses.edx.org/courses/course-v1:RITx+CYBER501x+1T2020/jump_to_id/b7f81698cf5949b1a9bbe7bd0114f287)

The CIA, Central Intelligence Agency, is the United States Service that gathers, processes,

and analyzes national security information from around the world.

How fitting that we can use the letters differently to represent the CIA model,

which describes three important goals for cybersecurity.

The C stands for confidentiality.

Cybersecurity requires privacy in data and information.

Certain people, devices, or processes should be permitted or restricted from seeing data, files,

and items, like username, password combinations.

Confidentiality is concerned with simply viewing data or information.

If the wrong people see data or information,

and they're not authorized, many problems could arise.

Company secrets, source code,

personal identifiable information and more, should be safeguarded.

The main way confidentiality is accomplished is through encryption,

which we'll cover in a future module.

The I in this CIA model stands for integrity.

Cybersecurity requires us to feel safe that data transmitted, processed,

and stored has not been changed from its original form,

either accidentally or maliciously.

If one bit of a message is changed, the whole message could change!

The difference between the words, hired and fired, that's one character!

But those words mean very different things.

Furthermore, the whole message itself could be corrupted and unreadable.

The main way integrity is accomplished is through hashing,

which we'll also cover in a future module.

The last letter of CIA, the A, stands for availability.

With all your cyber security measures in place, dealing with hardware, software, people,

processes, and more, users who are authorized to do their jobs should be able to do so.

You want to make sure that you don't fall victim to a

distributed denial of service, DDos, attack

and that you have full tolerance and load balancing

in the event of a cybersecurity incident or disaster.

[The AAA Model: Authentication](https://courses.edx.org/courses/course-v1:RITx+CYBER501x+1T2020/jump_to_id/b5bd39d62c264e8abe855d754ee0f68d)

Another important cybersecurity model is the AAA or triple A model,

which doesn't have anything to do with the American Automobile Association.

The first A refers to authentication, which is the process

of proving you are who you say you are.

When you claim you are someone, that's called identification.

When you prove it, that's authentication.

If I drove from Rochester to Canada and told the border patrol, "I'm Jonathan S. Wiseman,

let me into Canada," I would get some strange looks at the very least.

Authentication requires proof in one of three possible forms: Something you know,

like a password; something you have, like a key fob; something you are -- biometrics.

When you combine more than one of these categories,

that's called multifactor authentication, and that really is the future of authentication.

Multifactor authentication makes it really hard to authenticate

as someone else -- impersonating them.

Because if a hacker steals your password, he'd also have to possess a small key fob with a code

that rotates in parallel with code on the server you're logging into.

Or he'd need your iris, retina, or hand geometry.

Using two passwords is not multifactor authentication because they both fall

under the same something you know category.

It's like putting two locks on your door at home that could be opened with the same key.

There was a belief at some point that biometrics would simply replace passwords.

But especially with all the data breaches in recent years,

it's very clear that while you can change your password,

you simply cannot change your biometrics.

If your biometrics are stolen, then what?

You also lose anonymity when using credentials that are directly tied to you.

Your profile can easily be constructed, tied to all your actions,

linking together everything you do and everywhere you go in cyberspace.

Not that sharing credentials is necessarily a good thing, but if you temporarily had to,

for instance, in an emergency situation

and biometrics was the only option, then what would you do?

What happens when you grow a beard and the biometric authentication fails?

False positives and false negatives are legitimate issues

and could restrict or even allow access in error.

These are the most compelling arguments for a combination of authentication methods known

as 2FA or two-factor authentication.

Many companies like Google, LinkedIn,

and banks have recently enabled their sites for this 2FA system.

Sending codes to your phone through SMS, short message service -- text messages --

you use these codes that are texted to your phone in addition

to a password to access an account.

NIST, the National Institute of Standards

and Technology subsequently denounced two-factor authentication through text messages.

They stated that 2FA with SMS should be deprecated immediately due to the fact

that SMS messages can be intercepted or redirected.

NIST recommended other options like Google authenticator or even certain USB dongles.

However, Google, Twitter, Facebook, and tons

of other major websites are still using text messages for two-factor authentication today.

NIST's demand at least to this point has been completely ignored

by both companies and their users.

[The AAA Model: Authorization](https://courses.edx.org/courses/course-v1:RITx+CYBER501x+1T2020/jump_to_id/c511ef4a49b1413da7f1fd5b5de520bb)

The second A in the AAA model refers to authorization.

All right, the user has gone through identification

to say he is someone and authentication to prove it.

Now what? Do we let him see anything he wants?

Do we let him do anything he wants?

Authorization means that based on the user's credentials, we let him do certain things,

we let him see certain things but not others.

This is tied into the principle of least privilege, which states users and even devices,

programs, and processes should be granted enough permissions

to do their required functions and not a single drop more.

Any authorization beyond normal job functions opens the door for either accidental

or malicious violations of confidentiality, integrity, and availability.

This is specifically why the recommendation is to never use an administrator or a root account

on a system but rather an account with limited privileges.

If your system gets infected with malware, it will run with the privileges of the user.

Your account is granting authorization beyond that principle of least privilege.

Of course, you can escalate your privileges when necessary

or even use temporarily an administrator account,

but this way, at least, it's not constant.

[The AAA Model: Accounting](https://courses.edx.org/courses/course-v1:RITx+CYBER501x+1T2020/jump_to_id/a9538359be8e41128684d0aec6733a7a)

The third A in the AAA model refers to accounting.

Keeping track of users and their actions is very important.

From a forensics perspective, tracing back to events leading

up to a cybersecurity incident can prove very valuable to an investigation.

Predicting what disgruntled employees might be up to, for example, with a certain number

of failed login attempts to a server they are not authorized

to access is made possible by accounting.

A generic account for administrators or managers to share is not a very good idea.

The accounting can't tie actions to an individual.

The band The Police said it best, "Every move you make, I'll be watching you."

Some companies that send employees on mandatory vacations claim they do

so to avoid employee burnout; however when employee B steps

into employee A's role while employee A is on the beach in Hawaii,

employee B is performing checks and balances on employee A. Employee A could have been hiding

or covering up log entries that are now able to be seen and revealed by employee B

who is on the same level as employee A.

[Security vs. Convenience](https://courses.edx.org/courses/course-v1:RITx+CYBER501x+1T2020/jump_to_id/dbb10aa2596141dba192a13f7aec3390)

I also like to think of cybersecurity as a seesaw.

On one side you have security, and on the other side, convenience.

When one side goes up, the other side goes down.

Cybersecurity professionals have to figure out happy mediums to balance the seesaw.

If you make one side too high, the other suffers.

If you have little to no security implemented, users don't have to worry

about things like authentication.

But where would you be then?

If you have security measures that are unduly high, you risk employees not being able

to perform their jobs or even worse, trying to circumvent security perhaps by writing passwords

down and putting them on sticky notes on the monitors or under the keyboards.

It's a pain to take off a hat, a jacket, and shoes at the airport,

but I feel safer on the plane knowing everyone else did so, too.

Cybersecurity involves the same tradeoff.

[Threat Agents](https://courses.edx.org/courses/course-v1:RITx+CYBER501x+1T2020/jump_to_id/c44590faee6b4dbe9296a62c2dd8fc52)

From a cybersecurity perspective, you are looking to protect assets --

things that have value to a company.

They could be physical hardware, logical software, data, information,

company trade secrets, and even employees.

A threat is a looming danger that can change or damage your assets.

Think of the actual actions like fires, floods, hackers getting into your network,

malware infecting your systems, your server crashing without backups to go to,

or even a cleaner accidentally pulling out the plug to an important server.

Threat agents or actors are the ones carrying out the threats.

Yes, hackers are the first things that come to mind, but Mother Nature through earthquakes,

tornadoes, fires, and floods is also a threat agent.

A vulnerability is a weakness, a flaw in a program, device, network, and even a person.

Weak authentication checks, default user name password combinations,

incorrectly configured firewalls, and even a gullible

or naive employee are all vulnerabilities.

When threat actors carry out the threat, they exploit the vulnerability.

Exploit can be a verb meaning penetrating a system to exploit, or a noun meaning the tool

or method used to penetrate a system and exploit.

Interestingly enough, exploits are usually named after the vulnerability they exploit.

For example, MS08067 is a famous exploit from 2008 that allowed hackers to gain control

of a Windows XP or a Windows Server 2003 system.

Any systems running Windows XP today are vulnerable to that exploit.

Incredibly enough, Windows XP still has close to 10% market share,

even without security updates from Microsoft.

Hackers like to go after the low-hanging fruit first, and this is a prime example.

Risk is the combination of the probability of an event or loss from zero

to 100% and its consequence or impact.

For example, if your users' passwords are stored in plain text, the actual passwords

and not hashed as we'll see a future module, there's a high risk

that a data breach could result in those accounts being hacked.

You could suffer loss of reputation and customer goodwill --

for some companies that could be fatal.

There are three things that can be done to risk but eliminate is not one of them.

You could reduce or mitigate the risk.

We can eliminate some vulnerabilities and block some threats,

but nothing is ever going to be 100%.

Encryption, hashing, VPN's, firewalls, intrusion detection

and prevention systems, and more can reduce the risk.

Another thing you can do to risk is transfer it.

You can purchase cybersecurity insurance, which is a growing industry now,

or even use cloud computing and another company's resources.

Your cloud provider is now responsible for securing your data.

Last but not least, we can accept the risk.

Does the cost to protect a resource outweigh the cost of losing it or even replacing it?

If so, accepting the risk might make the most sense.

Before you spend your time and money, ask yourself the following questions:

What are the critical assets; what business processes require these assets;

what could interfere with normal operations; what are the risks;

which ones present the highest and most negative outcomes and should be prioritized;

given a range of solutions, which is the most cost-effective way of reducing the risks?